



Set Up Your PIX Security Appliance

[Home](#) > [Work With My Security Devices](#) > [Cisco Security Appliances](#) > [Set Up Your PIX Security Appliance](#)

Configure the PIX Security Appliance with PIX Device Manager

Step 1: [SMB Support Assistant Site Survey](#)

Step 2: [Set Up Your PIX Security Appliance Hardware](#)

Step 3: [Prepare to Configure Your PIX Security Appliance](#)

Step 4: Configure Your PIX Security Appliance with PIX Device Manager

[Introduction](#)

[Requirements](#)

[Connect to the PIX](#)

[Configure the PIX with the Startup Wizard](#)

[Basic Configuration](#)

[Outside Interface Configuration](#)

[Easy VPN Remote Configuration](#)

[Auto Update Configuration](#)

[Other Interfaces Configuration](#)

[NAT and PAT Configuration](#)

[DHCP Server Configuration](#)

[Create an Administrative Account](#)

[Configure Authentication/Authorization](#)

[Configure a Time Server](#)

[Next Step](#)

[Troubleshoot the Procedure](#)

[Related Information](#)

Step 5: [Configure the PIX Security Appliance with Adaptive Security Device Manager](#)

Step 6: [Set Up Internet Security on the PIX Security Appliance](#)

Introduction

This document describes how to configure the PIX Security Appliance with PIX Device Manager.

[Back to Top](#)

Service Requests

[Open a service request](#)

[Update a service request](#)

Feedback

Please rate this site:

++ + +/- - --

Suggestions for improvement:

Download PDF

[Step 4: Configure the PIX Security Appliance with PIX Device Manager](#)

[Set Up Your PIX Security Appliance](#)

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full Name:

Email:

Requirements

This section lists the items that you need, to use the PIX Device Manager (PDM) to access and configure your PIX:

- Ensure that your PIX 506E/515E is connected properly to your PC. If you have not installed your PIX hardware, refer to [Hardware Setup Procedure for the PIX Security Appliance](#) for instructions.
- A [straight-through Ethernet cable](#).
- Complete the [Prepare to Configure Your PIX Security Appliance](#) document
- Complete the Worksheets as instructed in the [Site Survey](#) namely:
 - Security Appliance Worksheet
 - Internet Worksheet
 - LAN Addressing Worksheet
- One of these web browsers:
 - Netscape version 7.1 or later
 - Internet Explorer version 5.5 or later
- Ensure that JavaScript and Java are enabled in your web browser and they are of the correct version. For more information see [Enable Java and JavaScript on Your PC](#).

[Back to Top](#)

Connect to the PIX

The PIX 506E/515E contains the integrated utility PDM. PDM is a browser-based tool designed to help you to set up, configure, and monitor the PIX Security Appliance. The PDM is preinstalled on the PIX 506E/515E.

Complete these steps to access the PIX with PDM:

1. Use an Ethernet cable to connect your PC to the inside port (Ethernet 1) on the rear panel of the PIX Security Appliance.
2. Change the PC IP address to match the PIX inside interface IP address (for example, if the PIX has an IP address 192.168.10.1, then configure your PC with 192.168.10.50 and with subnet mask 255.255.255.0).

Note: You may need to restart your computer after you change the IP address.

3. Check the ACT LED on the PIX front panel to verify that your PC has the basic connectivity to the inside port-Ethernet 1. When the connectivity occurs, the ACT LED on the front of the PIX lights up solid green.
4. Open a browser window and type **https:// <pix_interface_ip_address>** in your browser address field. This new IP address is

found on line R12 of the Security Appliance Worksheet.

Note: Ensure that you add the "s" to "https" to launch the web browser. HTTPS (HTTP over SSL) provides a secure connection between your browser and the PIX Security Appliance.

5. Leave both the user name and password boxes empty and press **Enter**.
6. Accept the security certificates.

To avoid the certificate from appearing in Windows Internet Explorer when the certificate dialog (titled "**Security Alert**") is shown, perform these steps:

- a. Click **View Certificate**.
 - b. Click **Install Certificate**.
 - c. Click **Next > Next > Finish > Yes**.
 - d. Click **OK** in the certificate dialog box.
 - e. In the Security Alert dialog box, click **Yes**.
7. The next logon screen appears. If no password is set, click **OK** to continue.
 8. Answer **`Always`** to the Security Warning asking "Do you want to install and run `Cisco PIX Device Manager`". PDM starts after the certificates are accepted.

[Back to Top](#)

Configure the PIX with the Startup Wizard

The Startup Wizard starts immediately the first time you connect to the PDM. You can access the Startup Wizard at any time through the Wizards menu. The Wizard can be aborted at any time by clicking Cancel. This preserves your original PIX settings. The Back button allows you to go back and change the information on previous screens before you click Finish.

Follow these steps to go through the initial setup of the PIX firewall:

Basic Configuration

On the Basic Configuration panel, configure the host name of your firewall and set the Enable Password, as well as a domain name for the firewall.

Follow these steps for the basic configuration panel:

1. Enter the Host Name from line B63 of your Internet Worksheet. The PIX Host Name can be up to 63 alphanumeric characters of mixed case.

Startup Wizard

Basic Configuration

Please specify the host name for the PIX. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to enter the device name given to you by your ISP as your firewall Host Name.

PIX Host Name:

Domain Name:

Enable Password

The Enable Password is used to administer the firewall by PDM or the Command Line Interface (CLI).

(Change Enable Password)

Old Enable Password:

New Enable Password:

Confirm New Enable Password:

< Back Next > Finish Cancel Help

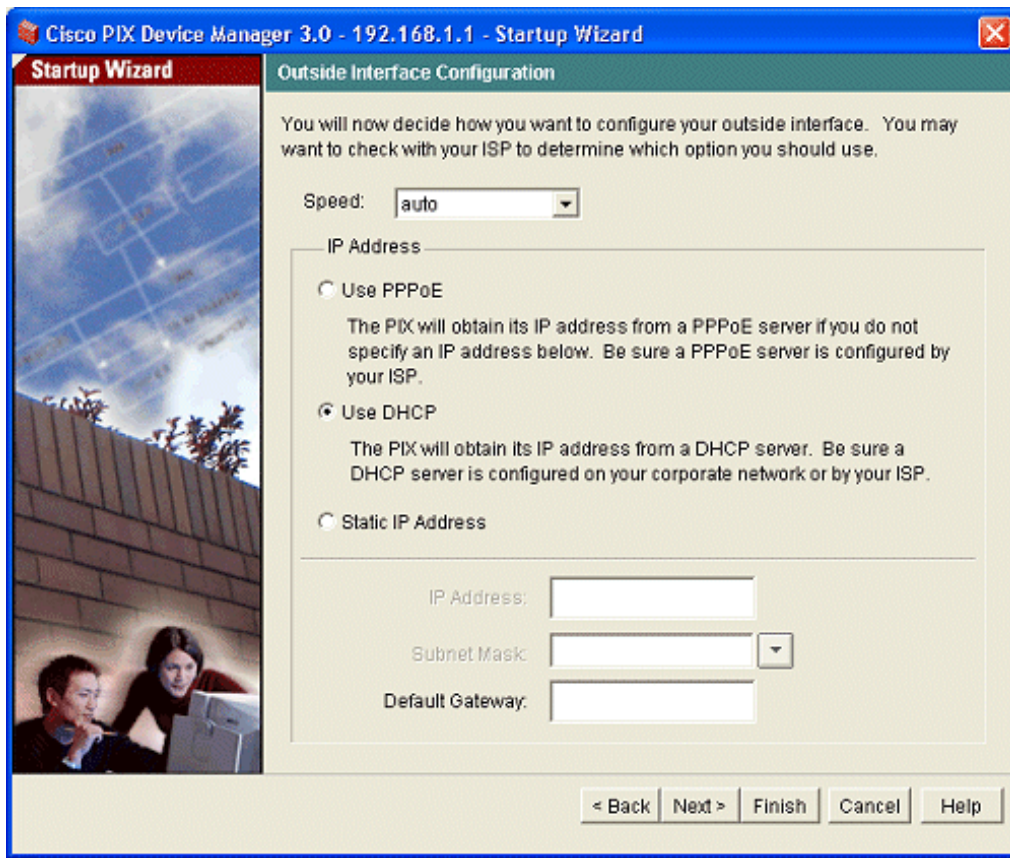
2. Enter the domain name the of the PIX Firewall found on line B48 of the Internet Worksheet. There is a 64 alphanumeric character limit on the domain name. No special characters or spaces must be used.
3. Check the box Change Enable Password.
4. Leave the Old Enable Password field blank. Enter the New Enable password. The password is case-sensitive and up to 16 alphanumeric characters. This password is found on line B12 of the Internet Worksheet.
5. Enter the password for the second time in the Confirm New Enable Password box.
6. Click **Next**.

Outside Interface Configuration

On the Outside Interface Configuration panel, configure the outside interface IP address, subnet mask, and default gateway.

Follow these steps to configure the outside interface:

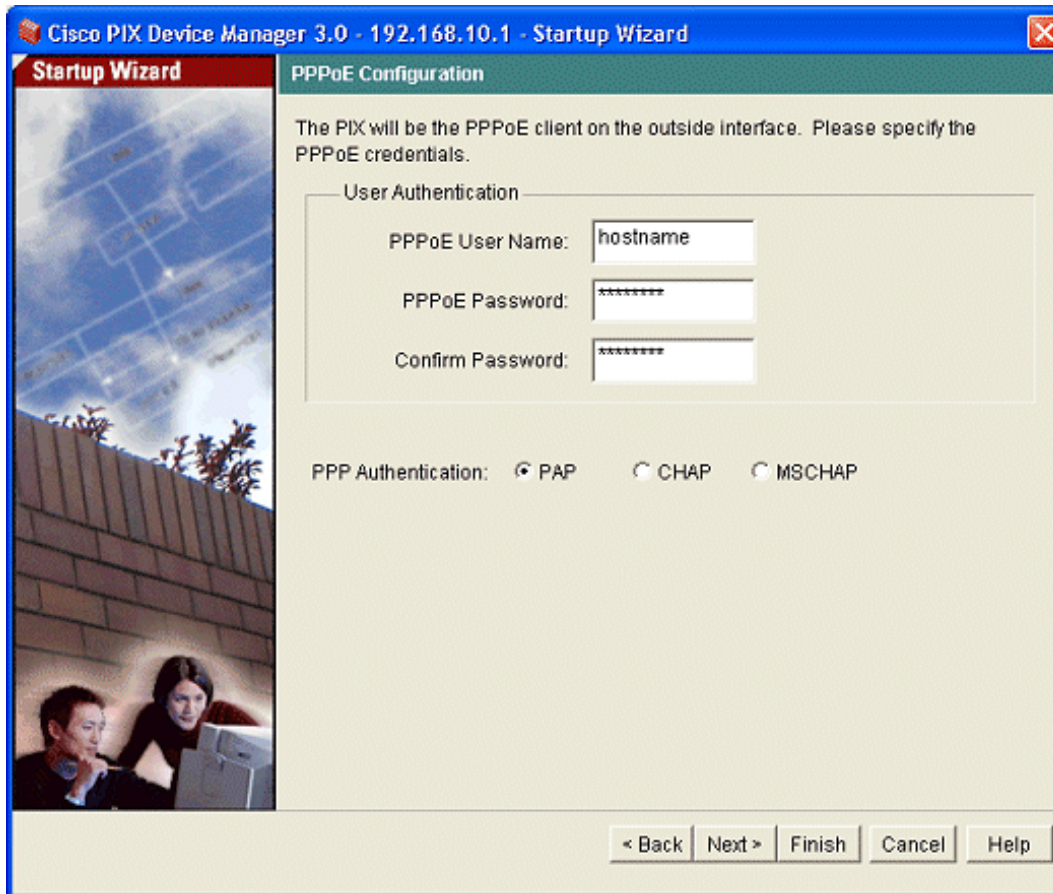
1. Speed—Leave the speed set to auto.



2. To configure the outside interface IP, follow these steps:

- If you select DHCP on the Internet Worksheet:
 - Click **Use DHCP**.
 - Click **Next**.
- If you select Static IP on the Internet Worksheet:
 - Click **Static IP Address**.
 - Enter the IP address from line B46 of the Internet Worksheet.
 - Enter the subnet mask found on line B41 of the Internet Worksheet.
 - Enter the gateway IP address found on line B47 of the Internet Worksheet.
 - Click **Next**.
- If you select Static PPP on the Internet Worksheet:

- Click **Use PPPoE**. The PPPoE Configuration screen appears.
- Enter the User Name (Remote Host Name) from line B63 of the Internet Worksheet.
- Enter the PPPoE password (Shared Secret) from line B64 of the Internet Worksheet.
- Enter the password again in the Confirm password box.
- Click the PPP authentication from line B62 of the Internet Worksheet.
- Click **Next**.



The screenshot shows the 'Startup Wizard' window for 'Cisco PIX Device Manager 3.0 - 192.168.10.1'. The window is titled 'PPPoE Configuration' and contains the following text: 'The PIX will be the PPPoE client on the outside interface. Please specify the PPPoE credentials.' Below this, there is a 'User Authentication' section with three input fields: 'PPPoE User Name:' containing 'hostname', 'PPPoE Password:' containing '*****', and 'Confirm Password:' containing '*****'. At the bottom of the form, there are three radio buttons for 'PPP Authentication': 'PAP' (selected), 'CHAP', and 'MSCHAP'. At the bottom right of the window, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Easy VPN Remote Configuration

On the Easy VPN Remote Configuration screen, follow these steps:

Ensure the box Enable Easy VPN Remote is not checked.

Cisco PIX Device Manager 3.0 - 192.168.1.1 - Startup Wizard

Startup Wizard

Easy VPN Remote Configuration

The PIX can act as an Easy VPN Remote device, enabling simplified deployment of VPNs to remote locations. The PIX can form a secure VPN tunnel with a Cisco VPN 3000 Concentrator, IOS-based router, or firewall acting as an Easy VPN Server and dynamically downloading additional VPN policy settings. Please make sure the Group and User information you enter below matches the information configured on your Easy VPN Server.

Enable Easy VPN Remote

Mode

If you will be using the DHCP server on the PIX to provide IP addresses to the hosts on your inside network, select Client Mode. If the hosts has static IP addresses, select Network Extension Mode.

Client Mode Network Extension Mode

Use Group Password

Group Name:

Group Password:

Confirm Password:

Primary EasyVPN Server:

Secondary EasyVPN Server:

User Name:

User Password:

Confirm Password:

Use X.509 Certificate

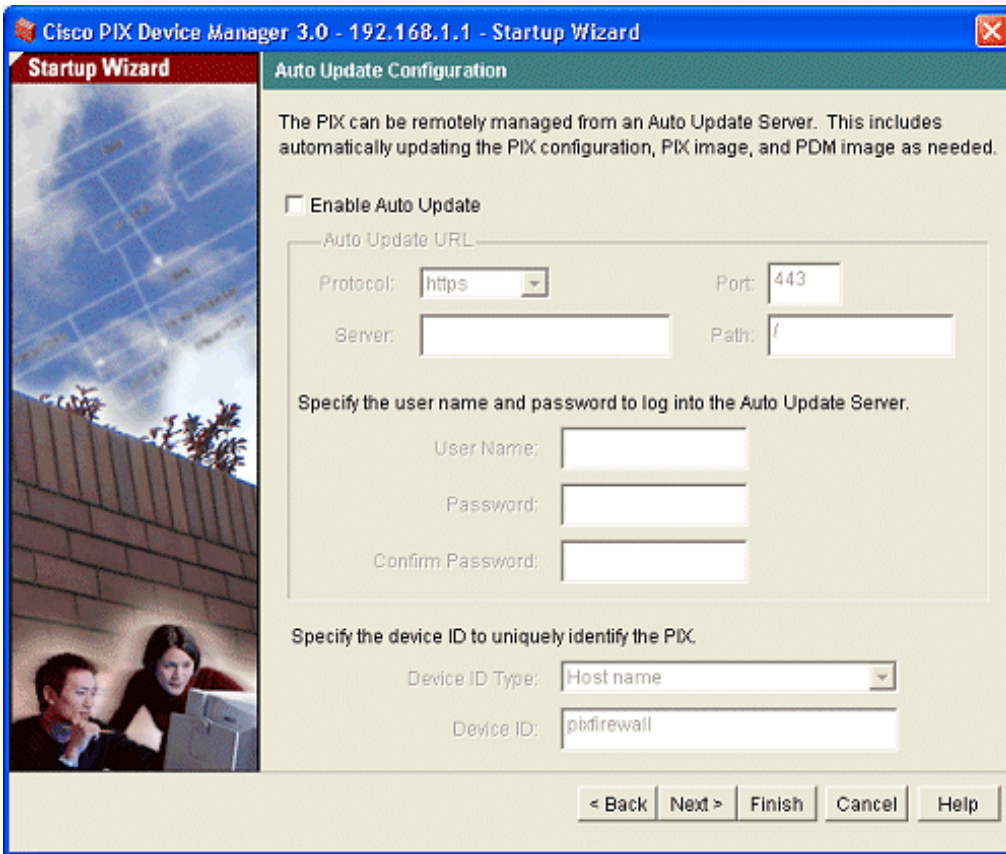
< Back Next > Finish Cancel Help

Click **Next**.

Auto Update Configuration

On the Auto Update Configuration screen, follow these steps:

Ensure that the check box Enable Auto Update is not checked.



The screenshot shows the 'Auto Update Configuration' window in Cisco PIX Device Manager 3.0. The window title is 'Cisco PIX Device Manager 3.0 - 192.168.1.1 - Startup Wizard'. The main heading is 'Auto Update Configuration'. Below the heading, there is a paragraph explaining that the PIX can be remotely managed from an Auto Update Server. A checkbox labeled 'Enable Auto Update' is currently unchecked. Below this, there is a section for 'Auto Update URL' with fields for Protocol (set to 'https'), Port (set to '443'), Server, and Path (set to '/'). There is also a section for specifying the user name and password to log into the Auto Update Server, with fields for User Name, Password, and Confirm Password. At the bottom, there is a section for specifying the device ID to uniquely identify the PIX, with a dropdown for Device ID Type (set to 'Host name') and a text field for Device ID (set to 'pixfirewall'). Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Startup Wizard

Auto Update Configuration

The PIX can be remotely managed from an Auto Update Server. This includes automatically updating the PIX configuration, PIX image, and PDM image as needed.

Enable Auto Update

Auto Update URL

Protocol: Port:

Server: Path:

Specify the user name and password to log into the Auto Update Server.

User Name:

Password:

Confirm Password:

Specify the device ID to uniquely identify the PIX.

Device ID Type:

Device ID:

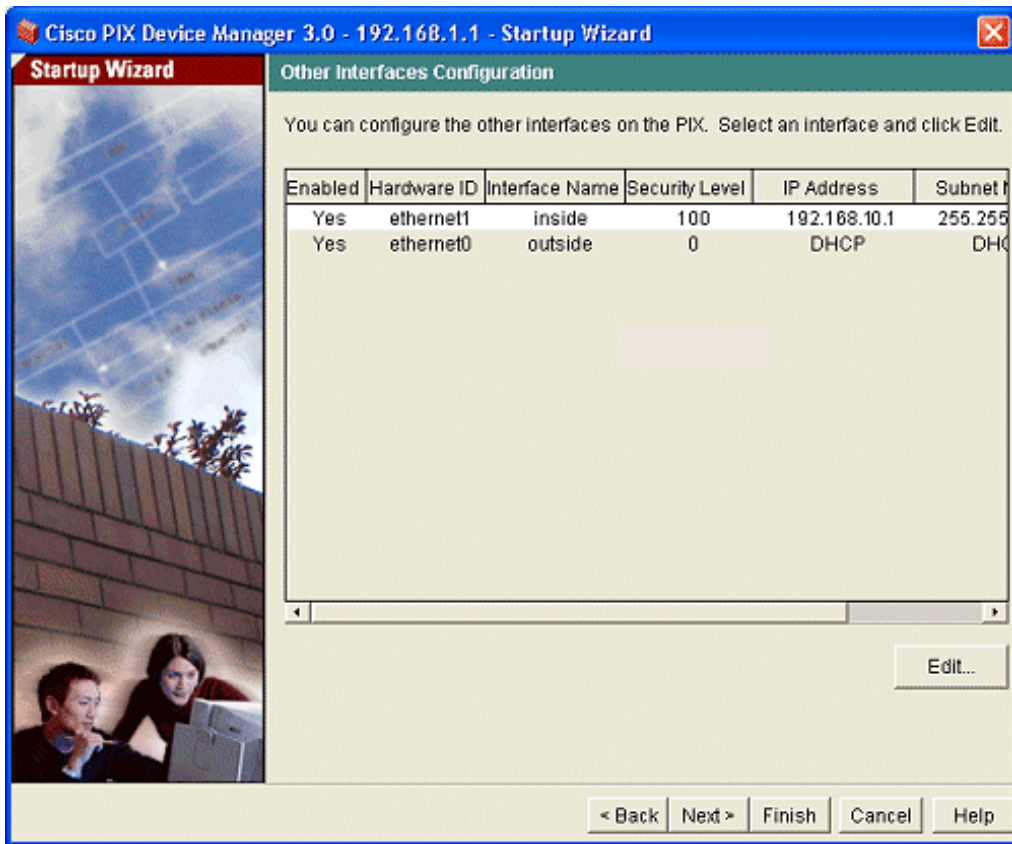
< Back Next > Finish Cancel Help

Click **Next**.

Other Interfaces Configuration

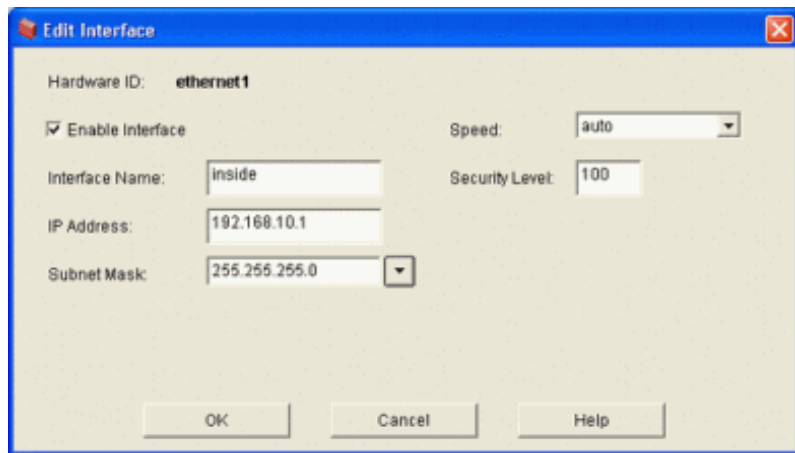
The Other Interfaces Configuration panel lets you to configure the IP addresses of the inside interface on the firewall. PDM automatically lists the interfaces available for configuration. In this panel you can set the IP address, speed, interface name, and security level to make each inside interface unique.

To configure the internal interfaces, follow these steps:



Highlight the preferred inside interface and click **Edit**. Another panel appears with the highlighted information.

- Ensure that the Enable Interface box is checked.
- Ensure the speed is set to Auto.
- Set the Security Level to 100.



Hardware ID: ethernet1

Enable Interface Speed: auto

Interface Name: inside Security Level: 100

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

OK Cancel Help

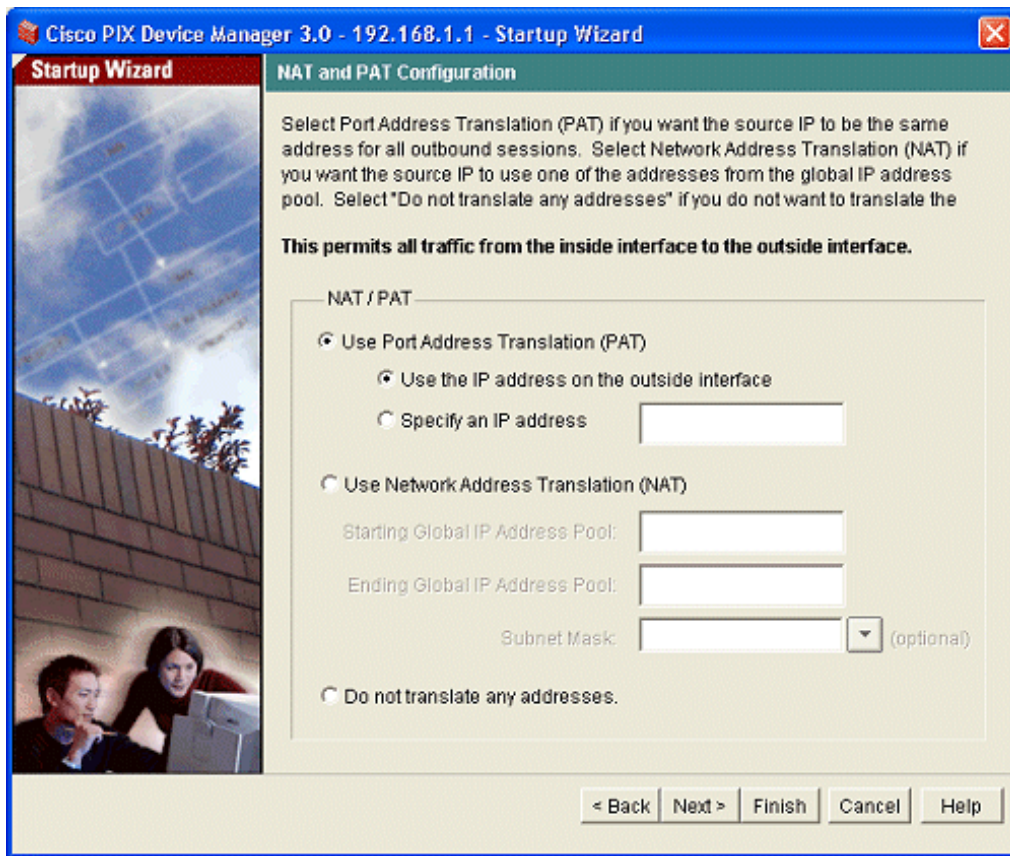
Click **OK** and click **Next**.

NAT and PAT Configuration

On the NAT and PAT Configuration panel, configure the Port Address Translation (PAT) to protect your network.

Follow these steps to configure PAT Configuration:

1. Select **Use Port Address Translation**.



2. Click **Use the IP address on the outside interface.**
3. Click **Next.**

DHCP Server Configuration

The DHCP Server Configuration panel lets you to configure the firewall as a DHCP server to clients on the inside interface. You can configure a range of IP addresses in the address pool to be assigned to the clients upon their request.

If line L3 on the LAN Addressing Worksheet is your PIX firewall, the DHCP server needs to be enabled. If not skip this step and click **Next.**

Follow these steps to configure the DHCP server:

1. Check **Enable DHCP on inside interface.**

Cisco PIX Device Manager 3.0 - 192.168.1.1 - Startup Wizard

Startup Wizard

DHCP Server Configuration

The PIX can be a DHCP server and provide IP addresses to the hosts on your inside network. To configure the DHCP server on another interface besides the inside interface, please use the PDM application.

Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: 192.168.10.50

Ending IP Address: 192.168.10.250

DHCP Parameters

DNS Server 1: 198.6.1.1 WINS Server 1:

DNS Server 2: 198.5.1.1 WINS Server 2:

Domain Name: company.com Lease Length: 3600 secs

< Back Next > Finish Cancel Help

2. Next to the DHCP Address Pool:
 - a. Enter the starting range of the DHCP server pool from line L50A on the LAN Addressing Worksheet.
 - b. Enter the ending range of the DHCP server pool from line L51A on the LAN Addressing Worksheet.
3. Next to the DHCP Parameters:
 - a. Enter the IP address of the DNS server from line L4A on the LAN Addressing Worksheet.
 - b. Enter the IP address of the alternate DNS server from line L5A on the LAN Addressing Worksheet.
 - c. Enter the domain name of the DNS server from line B48 of the Internet Worksheet.
4. Click **Next**.

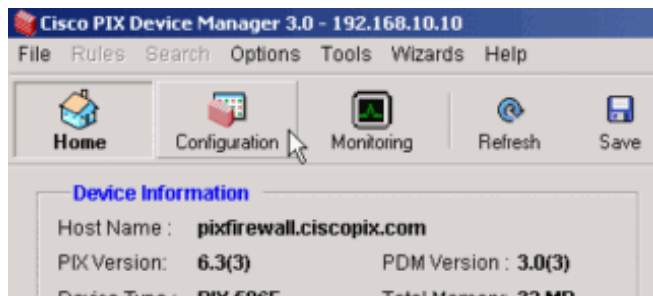
The create an Administrative Account panel appears. Click **Finish** to save the configuration to the PIX Security Appliance.

[Back to Top](#)

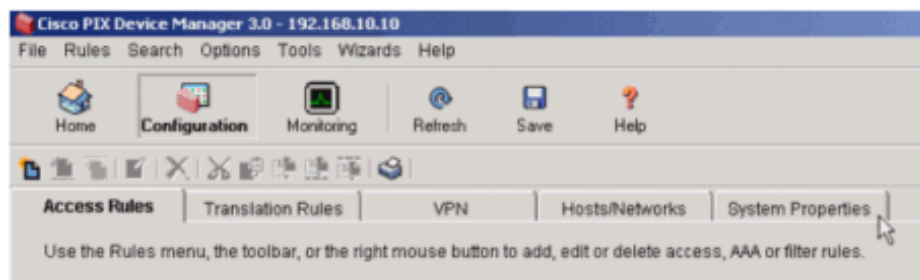
Create an Administrative Account

To create an administrative account to manage the PIX, follow these steps:

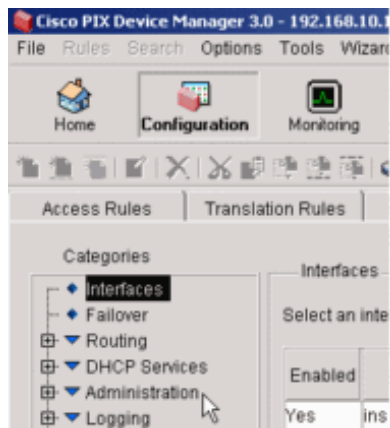
1. Click **Configuration**.



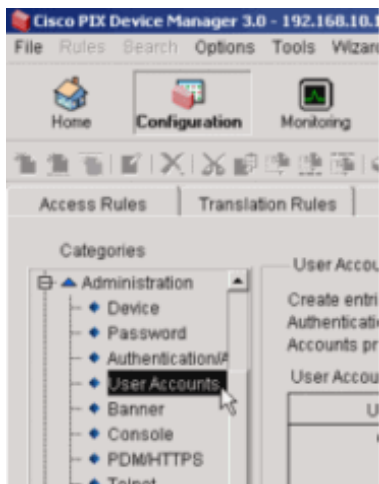
2. Click **System Properties**.



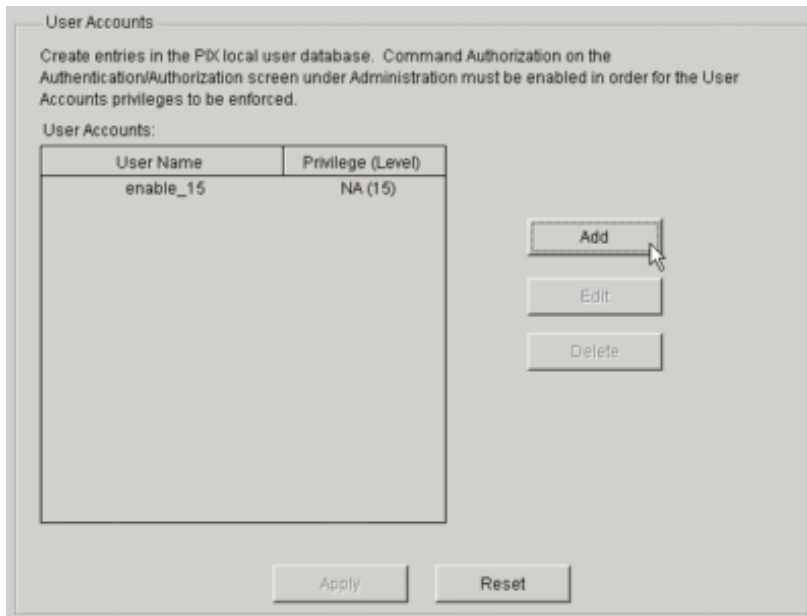
3. Click **Administration**.



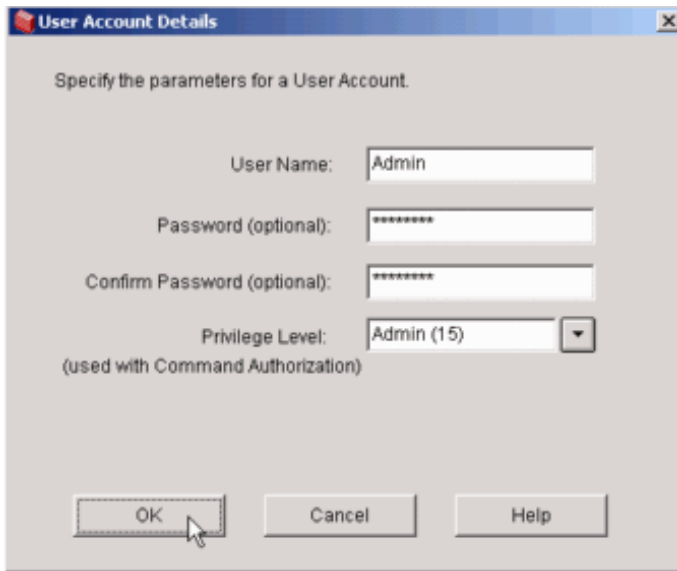
4. Click **User Accounts**.



5. Click **Add**.



6. Type **admin** in the User Name field and enter the password that you entered on the Internet Worksheet (B11) in the Password and Confirm Password fields. Ensure that the Privilege Level is set to **15** and click **OK**.



7. Click **OK** in the **Information** window.



8. Click **Apply**.

User Accounts

Create entries in the PIX local user database. Command Authorization on the Authentication/Authorization screen under Administration must be enabled in order for the User Accounts privileges to be enforced.

User Accounts:

User Name	Privilege (Level)
enable_15	Admin (15)
Admin	Admin (15)

Add

Edit

Delete

Apply

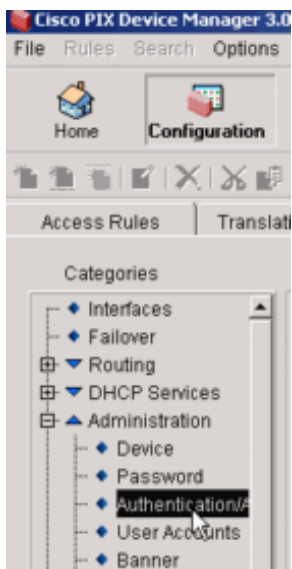
Reset

[Back to Top](#)

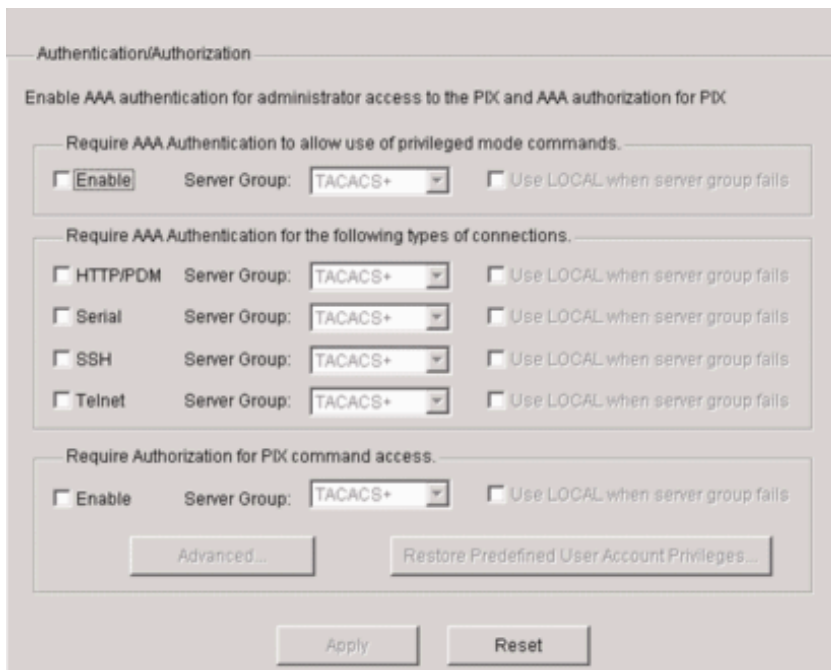
Configure Authentication/Authorization

To configure authentication or authorization, follow these steps:

1. Click **Configuration > System properties > Administration > Authentication/Authorization**.

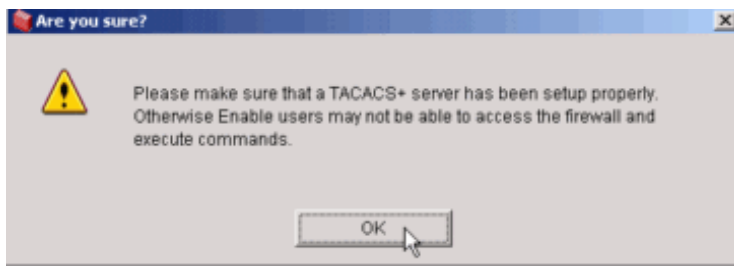


The Authentication/Authorization screen appears:



2. In the Authentication/Authorization screen, make these changes:

- a. Next to the Require AAA Authentication to allow use of Privileged mode commands, check the Enable check box.
- b. Click **OK** in **Are you sure?** window and select **LOCAL** from the Server Group.



- c. Next to Require AAA Authentication for the these type of connections, check the **HTTP/PDM** check box and select **Local**. Click **OK** to the Are you sure? warning message.
- d. Next to the Require Authorization for PIX commands access, check the **Enable** check box and then click **OK** in the warning message. Select **LOCAL** from the Server Group.

Authentication/Authorization

Enable AAA authentication for administrator access to the PIX and AAA authorization for PIX

Require AAA Authentication to allow use of privileged mode commands.

Enable Server Group: LOCAL Use LOCAL when server group fails

Require AAA Authentication for the following types of connections.

HTTP/PDM Server Group: LOCAL Use LOCAL when server group fails

Serial Server Group: TACACS+ Use LOCAL when server group fails

SSH Server Group: TACACS+ Use LOCAL when server group fails

Telnet Server Group: TACACS+ Use LOCAL when server group fails

Require Authorization for PIX command access.

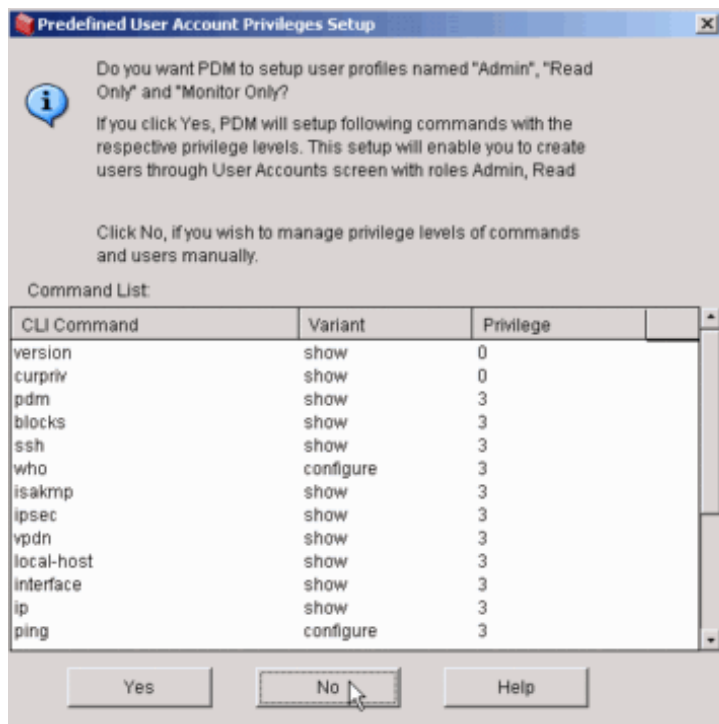
Enable Server Group: LOCAL Use LOCAL when server group fails

Advanced... Restore Predefined User Account Privileges...

Apply Reset

Click **Apply**.

The Predefined User Account Privileges screen appears.



Click **No**.

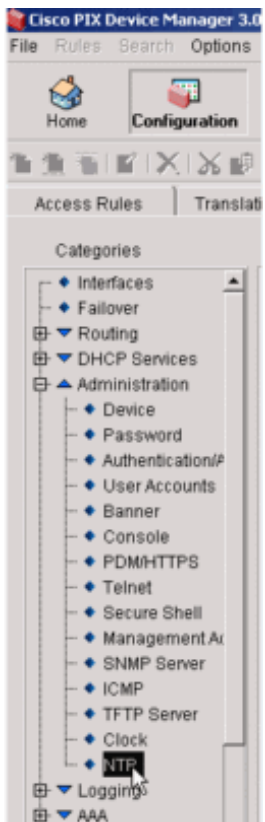
Note: If PDM displays a login window, log in with the new username and password.

[Back to Top](#)

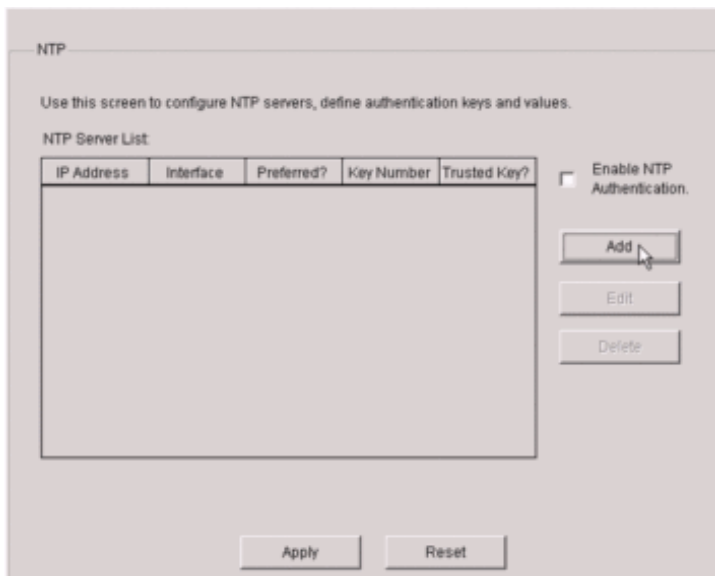
Configure a Time Server

Follow these steps to configure a time server on the security appliance:

1. Click **Configuration > System properties > Administration > NTP**.

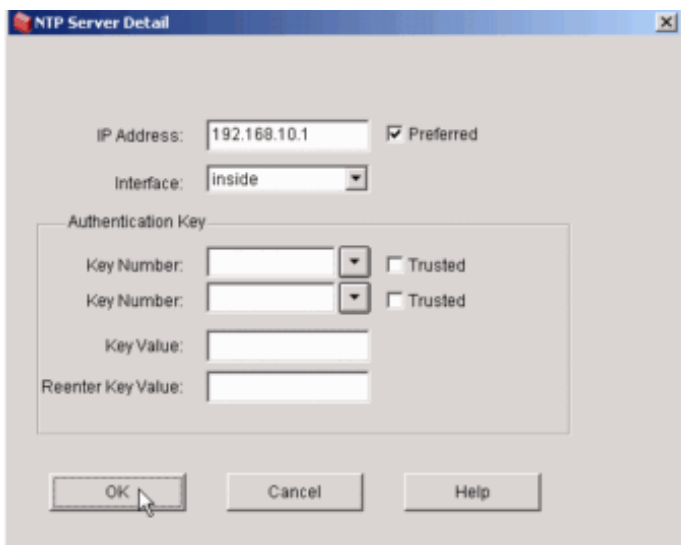


2. On the NTP screen, click **Add**.



3. In the **NTP Server Detail** window, enter these values:

- a. IP Address: Enter the IP address of the router than you entered in field L6A of the LAN Addressing Worksheet.
- b. Interface: **Inside**
- c. Check the check box Preferred.
- d. Leave the remaining fields blank.
- e. Click **OK**.



f. Click **Apply**.

NTP

Use this screen to configure NTP servers, define authentication keys and values.

NTP Server List:

IP Address	Interface	Preferred?	Key Number	Trusted Key?
192.168.10.1	inside	Yes		No

Enable NTP Authentication.

Add

Edit

Delete

Apply

Reset

- g. Click the **Save** button to save the configuration.



[Back to Top](#)

Next Step

You have completed the initial setup of the PIX Security Appliance.

Refer to [Set Up Internet Security on the PIX Security Appliance](#) to secure your PIX.

[Back to Top](#)

Troubleshoot the Procedure

This section provides information about common problems that you may encounter.

Problem	Condition	Suggested Solution(s)
If the Browser asks for acceptance of the security certificate again.	When the hostname or domain name is changed.	This is normal. Accept the security certificates again. (If you change the hostname or domain of the firewall unit, the browser asks you to accept the new security certificate.)
Browser asks for the password again.	<p>If you change the password on the firewall unit, the browser asks you to reenter the password for authentication.</p> <p>If you use the Java Plug-in, the browser prompts you for your username and password twice.</p>	Keep track of new and changed passwords on your worksheets.
Browser is unable to access PDM.	When you attempt to access PDM, the message "the page cannot be displayed" appears in Internet Explorer or the message "network connection was refused by the server" appears in Netscape Communicator.	Check that you are use " https " in your connection to "https:// <i>inside_interface_ip_address</i> " and not "http". The connection is not possible by "http," it must be " https ."
Help files appear corrupted (on Internet Explorer only).	This can occur because PDM compresses the online Help files and Internet Explorer requires HTTP 1.1 to be enabled to handle compressed files properly.	If you use a proxy server, select the Use HTTP 1.1 through proxy connections check box .
Some graphics or icons do not display properly.	PDM is made to run with a Java Plug-in that is not supported (PDM supports Java Plug-in 1.4.2).	<p>If you have the Java Plug-in installed, confirm that it is your default Java Virtual Machine (JVM). Follow these steps to ensure that the Java Plug-in is your default JVM:</p> <ol style="list-style-type: none"> 1. In Internet Explorer, click Tools > Internet Options. 2. Click the Advanced tab. Scroll down. Look for a Java (Sun) section. If there is one, confirm that Use Java 2 is selected.

		<p>In Netscape, click Edit > Preferences. Click Advanced. Make sure that the Enable Java Plug-in check box is selected.</p> <p>For more detailed instructions see Enable Java and JavaScript on Your PC.</p>
PDM launches slowly.	The startup speed of PDM depends on the amount of available RAM in your computer and whether virus scanning software runs on your computer.	<p>You can increase your available RAM by closing other applications.</p> <p>The time required to download the PDM applet can be greatly affected by the speed of the link between your workstation and the firewall unit. A minimum of 56 Kbps link speed is required. However, 3.84 Mbps or higher is recommended. Once the PDM applet is loaded on your workstation, the link speed impact on PDM operation is negligible.</p>
There is access only to the Monitoring tab in PDM.	The use of certain firewall CLI commands, and certain command combinations, limits the access in PDM to the Monitoring tab.	For more information on these commands and command combinations, see the <i>Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide Release 2.3</i> .
PDM prompts for the username/password and certificate information twice.	This is normal when you use Java Plug-in.	You can choose to accept the certificate permanently so that this dialog box does not appear again.

[Back to Top](#)

Related Information

- [Site Survey](#)
- [Set Up Internet Security on the PIX Security Appliance](#)

- [Enable Java and JavaScript on Your PC](#)
- [SMB Technical Assistance Center \(SMB TAC\)](#)